

SEALED

UNITED STATES DISTRICT COURT

FILED

for the

Northern District of Texas

March 22, 2023

KAREN MITCHELL

CLERK, U.S. DISTRICT  
COURT

In the Matter of the Search of  
(Briefly describe the property to be searched  
or identify the person by name and address)

Case No. 3:23-MJ-311-BH

a black Apple iPhone, assigned phone number  
(214) 624-2552

APPLICATION FOR A SEARCH WARRANT

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property (identify the person or describe the property to be searched and give its location):

See Attachment A.

located in the Northern District of Texas, there is now concealed (identify the person or describe the property to be seized):

See Attachment B.

The basis for the search under Fed. R. Crim. P. 41(c) is (check one or more):

- ☒ evidence of a crime;
- ☒ contraband, fruits of crime, or other items illegally possessed;
- ☒ property designed for use, intended for use, or used in committing a crime;
- ☐ a person to be arrested or a person who is unlawfully restrained.

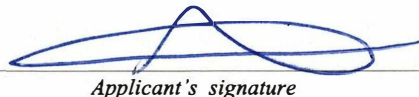
The search is related to a violation of:

Code Section	Offense Description
18 U.S.C. § 2252A(a)(5)	Possession of or access with intent to view child pornography

The application is based on these facts:

See attached affidavit of SA Ingri C. Hartwig, FBI.

- ☒ Continued on the attached sheet.
- ☐ Delayed notice of \_\_\_\_\_ days (give exact ending date if more than 30 days: \_\_\_\_\_) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.



Applicant's signature

SA Ingri C. Hartwig, FBI

Printed name and title

Agent sworn and signature confirmed via reliable electronic means, pursuant to Fed. R. Crim. P. 41(d)(3).

Date:

March 22, 2023



Judge's signature

City and state: Dallas, Texas

IRMA CARRILLO RAMIREZ, U.S. Magistrate Judge

Printed name and title

**AFFIDAVIT IN SUPPORT OF SEARCH WARRANT APPLICATION**

1. I, Ingri Hartwig, a Special Agent (SA) with the Federal Bureau of Investigation, being duly sworn, depose and state the following:

2. I am a Special Agent with the Federal Bureau of Investigation (FBI). I have been a Special Agent with the FBI since March 2009. I am currently assigned to the Dallas Division. As a federal agent, my duties include, but are not limited to, the investigation and enforcement of Title 18 of the United States Code (U.S.C.). I am an “investigative or law enforcement officer of the United States” within the definition in 18 U.S.C. § 2510(7), in that I am an agent of the United States authorized by law to conduct investigations of, and make arrests for, federal offenses.

3. I am currently assigned to a Child Exploitation Task Force, wherein some of my duties and responsibilities include investigating criminal violations relating to the sexual exploitation of children, such as the illegal production, transportation, distribution, receipt, and possession of child pornography, in violation of 18 U.S.C. §§ 2251, 2252, and 2252A. I have gained expertise in these types of investigations through training in seminars, classes, and my everyday work.

4. In addition, I have received training in the investigation and enforcement of federal child pornography laws and have had the opportunity to observe and review numerous examples of child pornography (as defined in 18 U.S.C. § 2256) in all forms of media, including computer media.

5. This affidavit is being made in support of a search warrant application under Rule 41 of the Federal Rules of Criminal Procedure. For the reasons set forth hereinafter, I submit

that there is probable cause to believe that a black Apple iPhone, assigned phone number (214) 624-2552 (the “**Target Device**”), which is in the lawful possession of the FBI, was used by **Paul Wayne Rigney**, a white male with date of birth 02/16/19XX and who is currently in federal custody (“**Rigney**”), to possess or access with intent to view child pornography in violation of 18 U.S.C. § 2252A(a)(5).<sup>1</sup> I submit there is also probable cause to believe that evidence of this crime will be found in the **Target Device**, which, as explained below, is **Rigney’s** cell phone. The application seeks authorization to search the **Target Device** itself for evidence of the above-described violation by **Rigney**. The **Target Device** is more fully described in Attachment A, and a description of the evidence to be seized from the **Target Device** is further described in Attachment B.

6. The information set forth in this affidavit comes from an investigation I have conducted, my training and experience, and information provided to me by other government and law enforcement officers. Since this affidavit is being submitted for the limited purpose of securing a search warrant, I have not included each and every fact known to me concerning this investigation. I have only set forth those facts that I believe are necessary to establish probable cause to believe that evidence of violations of 18 U.S.C. § 2252A, or the attempt to commit such violations, is presently located within the **Target Device**.

#### **DEFINITIONS**

7. The following definitions, inclusive of all definitions contained in 18 U.S.C. § 2256, apply to this affidavit and its attachments:

---

<sup>1</sup> **Rigney’s** year of birth is redacted to protect personal identifiable information.

a. “Computer” refers to any electronic, magnetic, optical, electrochemical, or other high-speed data processing device capable of performing logical or storage functions, and includes any data storage facility or communications facility directly related to such a device. As used herein, “computer” also incorporates digital devices that complete these same functions, such as smartphones, tablets, connected devices, and e-readers. *See* 18 U.S.C. § 1030(e)(1).

b. “Internet Protocol address” or “IP address” refers to a unique number used by a computer to access the Internet. IP addresses can be dynamic, meaning that the Internet Service Provider assigns a different unique number to a computer every time it accesses the Internet. IP addresses may also be static, which means the provider assigns a user’s computer a particular IP address that is used each time the computer accesses the Internet.

c. “Mobile applications” or “mobile apps” are computer programs or software applications specifically designed to run on mobile electronic devices (e.g., smartphones, tablets, e-readers, etc.). Mobile applications are generally downloaded from application distribution platforms operated by specific mobile operating systems, like App Store (Apple mobile devices) or Google Play Store (Android mobile devices).

d. “Instant messaging” is a type of communication that offers real-time text transmission over the Internet. Instant messaging generally involves short messages which are transmitted between two or more parties. Various social networking, dating, and gaming websites and mobile applications offer instant messaging for users to communicate amongst themselves. More advanced features of instant messaging include

push technology to provide real-time text, and the ability to send/receive digital files, clickable hyperlinks, and video chat.

e. The terms “records,” “documents,” and “materials,” as used herein, include all information recorded in any form, both visually or aurally, and by any means, whether in handmade form (including, but not limited to: writings, drawings, and paintings), photographic form (including, but not limited to: microfilm, microfiche, prints, slides, negatives, videotapes, motion pictures, and photocopies), mechanical form (including, but not limited to: phonograph records, printing, or typing), or electrical, electronic, or magnetic form (including, but not limited to: tape recordings, cassettes, compact discs, electronic, or magnetic storage devices such as floppy diskettes, hard disks, CD-ROMs, flash drives, digital video disks or DVDs, Personal Digital Assistants (PDAs), Multimedia Cards (MMCs), memory sticks, optical disks, printer buffers, smart cards, memory calculators, electronic dialers, electronic notebooks, as well as digital data files and printouts or readouts from any magnetic, electrical, or electronic storage device).

#### **FACTS IN SUPPORT OF PROBABLE CAUSE**

8. On May 24, 2022, pursuant to a state of Texas search warrant, members of the FBI Crimes Against Children Task Force executed a search at **Rigney’s** residence, located at 3225 Turtle Creek Boulevard, #543B, Dallas, TX. Several electronic devices were seized as a result of the search and submitted into evidence at the FBI Dallas Division.

9. I reviewed the results of the forensic examinations completed on each item seized from **Rigney’s** residence and found child pornography (as defined in 18 U.S.C. § 2256) on two of those devices.

10. On March 9, 2023, pursuant to an arrest warrant issued by the Northern District of Texas following indictment, **Rigney** was taken into custody on two counts of Possession of Child Pornography.

11. On Friday, March 10, 2023, **Rigney's** daughter, Charlotte Rigney, who also currently resides at 3225 Turtle Creek Boulevard, #543B, Dallas, TX, told the FBI that she had found child pornography on her father's cellular device, a black iPhone (the **Target Device**), which was not seized by the FBI during **Rigney's** arrest. I arranged with Charlotte Rigney to pick up the **Target Device** the following week. Charlotte Rigney informed me that another individual (a friend of **Rigney**) had a key to **Rigney's** residence and Charlotte Rigney was going out of town for the weekend before I would be picking up the **Target Device**. So I instructed Charlotte to lock the **Target Device** in a storage unit and not to examine it any further. Charlotte Rigney stated she would do this.

12. On March 14, 2023, I received the **Target Device** from Charlotte Rigney. In answering my questions, she stated she had seen prepubescent girls with their genitals exposed in the photo gallery of the **Target Device** after she had answered a phone call on the **Target Device**. Charlotte Rigney said she knew her father's telephone number to be (214) 624-2552 and provided the passcode to the **Target Device** as "66401."

13. The **Target Device** is currently in the evidence control room at the FBI. In my training and experience, I know that the **Target Device** has been stored in a manner in which its contents are, to the extent material to this investigation, in substantially the same state as they were when the **Target Device** first came into the possession of the **FBI**.

14. A search of law enforcement databases confirmed telephone number (214) 624-2552 is associated with **Rigney**, whose address is 3225 Turtle Creek Boulevard, #543, Dallas, TX. I thus believe the **Target Device** is **Rigney's** cellular phone.

#### **BACKGROUND ON COMPUTERS AND CHILD PORNOGRAPHY**

15. Based on my training and experience in child exploitation investigations, I am aware that computers, computer technology, and the Internet significantly facilitate the receipt, distribution, and possession of child pornography. Computers generally serve five (5) functions in connection with child exploitation offenses: production, communication, distribution, storage, and social networking. Child pornography offenders can transpose photographic images from a camera into a computer-readable format with a scanner. With digital cameras, the images can be transferred directly onto a computer. A modem allows any computer to connect to another computer through the use of telephone, cable, or wireless connection. A smartphone or other camera-equipped mobile device (e.g. tablet) is capable of not only producing child pornography images directly with the device's camera, but of also transmitting child pornography images via the use of the Internet. Therefore, through use of the Internet, electronic contact can be made to literally millions of computers, smartphones, and other wireless electronic devices around the world.

16. A computer's ability to store images in digital form makes the computer itself an ideal repository for child pornography. The size of the electronic storage media (commonly referred to as the hard drive) used in personal computers has grown significantly within the last several years. These drives can store thousands of images at very high resolution. In addition, electronic devices such as smartphones (e.g., Apple iPhones, Samsung Galaxy), connected



devices (e.g., Apple iTouch), e-readers, and tablets (e.g., Apple iPads, Kindle Fire) now function essentially as computers with the same abilities to store images in digital form.

17. The Internet affords collectors of child pornography and those with a sexual interest in children several different venues for obtaining, viewing, and trading child pornography in a relatively secure and anonymous fashion. Collectors and distributors of child pornography also use online resources to retrieve and store child pornography, including, but not limited to, services offered by Internet portals such as Yahoo, Outlook, and Google. These online services allow a user to set up an account with a remote computing service that provides e-mail services as well as electronic storage of computer files in any variety of formats. A user can set up an online storage account from any computer or device with access to the Internet, and evidence of such online storage of child pornography is often found on the user's computer or device.

18. Even when such files have been deleted, they can be recovered months or years later using readily available forensic tools. When a person deletes a file on a computer, the data contained in the file does not actually disappear; rather, that data remains on the hard drive until it is overwritten by new data. Therefore, deleted files, or remnants of deleted files, may reside on the hard drive in space that is not allocated to an active file for long periods of time before they are overwritten. A computer's operating system may also keep a record of deleted data in a "swap" or "recovery" file.

19. Additionally, a computer user's Internet activity generally leaves traces in a computer's web cache and Internet history files. Files that have been viewed on the Internet are automatically downloaded into a temporary Internet directory or "cache." Browsers typically



maintain a fixed amount of hard drive space devoted to these files, and the files are only overwritten as they are replaced with more recently viewed Internet pages. Therefore, the ability to retrieve residue of an electronic file from a hard drive depends less on when the file was downloaded or viewed, and more on the user's operating system, storage capacity, and computer habits.

### **BACKGROUND REGARDING SMARTPHONES AND MOBILE ELECTRONIC DEVICES**

20. Smart cellular telephones (smartphones), in addition to functioning as a handheld wireless electronic communication device capable of making and receiving telephone calls, can function as a video camera, a camera phone, a portable media player, and an Internet client with email and web browsing capabilities with Wi-Fi and cellular data connectivity. In addition to all of the above capabilities, smartphones also provide basic functions such as, but not limited to: (1) storing names and phone numbers in electronic "address books"; (2) sending, receiving, and storing text messages and email; (3) taking, sending, receiving, and storing still photographs and moving video; (4) storing and playing back audio files; (5) storing dates, appointments, and other information on personal calendars; (6) accessing and downloading information from the Internet; and (7) receiving, accessing, and storing voice mail. In addition, smartphones are capable of running applications such as Google Hangouts.

21. Smartphones are also designed to connect to personal computers to share files, share internet connections, perform backup functions, and charge the phone battery. Smartphone users commonly synchronize their data files, including image files, to personal computers to maintain a backup of these files.

22. Based on my training and experience, I am aware smartphones and other mobile electronic devices (e.g., tablets, e-readers, etc.) are fundamentally computers under 18 U.S.C. § 1030(e)(1), and are generally capable of acting as electronic storage devices. Furthermore, they are capable of connecting to computer networks, including the Internet, via cellular radio and/or Wi-Fi.

23. Based on my training and experience, I am aware that cellular phones today routinely have slots for external storage media, such as microSD cards, which can be removed and transferred to a computer for file sharing. I am aware that the storage capacity and features in smartphones on the market today also afford device users the ability to store large amounts of data, including, but not limited to image and video files, within the device's memory, applications, or SD cards. I am aware that smartwatches today have internal storage that allows the storage of files such as images and videos. I am also aware that smartwatches can stream and download contents from cellular devices they are synced to.

24. I also know, based on my training and experience, that modern cellular telephones are essentially computers with a smaller, pocket-sized footprint. They have advanced processors, high-definition displays, and mass data storage. High-end cellular phones can ship with up to 1 TB of data storage. As small computers, cellular telephones must be searched in a similar way to computers. Moreover, due to their portability, file system design, and mass data storage, files may be stored anywhere on the device. In my training and experience, users who possess, transport, receive, or otherwise traffic in child pornography will often hide files in unsuspecting locations on a cellular telephone to avoid detection by others. I have observed individuals using special applications designed specifically to encrypt and/or conceal their

contents for the purpose of hiding child pornography from law enforcement. Due to these factors, in addition to those reasons described below, I seek authorization to search the entire contents of the **Target Device** for evidence of child pornography.

### **BACKGROUND REGARDING FORENSIC ANALYSIS**

25. As noted above, electronic devices like cellular telephones can store information for long periods of time. Similarly, things that have been viewed via the Internet are typically stored for some period of time on the device. This information can sometimes be recovered with forensics tools.

26. As further described in Attachment B, this application seeks permission to locate not only electronically stored information that might serve as direct evidence of the crimes described on the warrant, but also forensic evidence that establishes how the **Target Device** was used, the purpose of its use, who used it, and when. There is probable cause to believe that this forensic electronic evidence might be on the **Target Device** because:

a. Data on the storage medium can provide evidence of a file that was once on the storage medium but has since been deleted or edited, or of a deleted portion of a file (such as a paragraph that has been deleted from a word processing file).

b. Forensic evidence on a device can also indicate who has used or controlled the device. This “user attribution” evidence is analogous to the search for “indicia of occupancy” while executing a search warrant at a residence.

c. A person with appropriate familiarity with how an electronic device works may, after examining this forensic evidence in its proper context, be able to draw

conclusions about how electronic devices were used, the purpose of their use, who used them, and when.

d. The process of identifying the exact electronically stored information on a storage medium that is necessary to draw an accurate conclusion is a dynamic process. Electronic evidence is not always data that can be merely reviewed by a review team and passed along to investigators. Whether data stored on a computer is evidence may depend on other information stored on the computer and the application of knowledge about how a computer behaves. Therefore, contextual information necessary to understand other evidence also falls within the scope of the warrant.

e. Further, in finding evidence of how a device was used, the purpose of its use, who used it, and when, sometimes it is necessary to establish that a particular thing is not present on a storage medium.

27. Based on the foregoing, and consistent with Rule 41(e)(2)(B), the warrant I am applying for would permit the examination of the **Target Device** consistent with the warrant. The examination may require authorities to employ techniques, including but not limited to computer-assisted scans of the entire medium, that might expose many parts of the device to human inspection in order to determine whether it is evidence described by the warrant.

28. Because this warrant seeks only permission to examine the **Target Device**, the execution of this warrant does not involve the physical intrusion onto a premises. Consequently, I submit there is reasonable cause for the Court to authorize execution of the warrant at any time in the day or night.

**BIOMETRIC ACCESS**

29. The warrant I am applying for would permit law enforcement to obtain from **Rigney** the display of physical biometric characteristics (such as fingerprint, thumbprint, or facial characteristics) in order to unlock the **Target Device** subject to search and seizure pursuant to this warrant. I seek this authority based on the following:

a. I know from my training and experience, as well as from information found in publicly available materials published by device manufacturers, that many electronic devices, particularly newer mobile devices and laptops, offer their users the ability to unlock the device through biometric features in lieu of a numeric or alphanumeric passcode or password. These biometric features include fingerprint scanners and facial recognition features. Some devices offer a combination of these biometric features, and the user of such devices can select which features they would like to utilize.

b. If a device is equipped with a fingerprint scanner, a user may enable the ability to unlock the device through his or her fingerprints. For example, Apple offers a feature called “Touch ID,” which allows a user to register up to five fingerprints that can unlock a device. Once a fingerprint is registered, a user can unlock the device by pressing the relevant finger to the device’s Touch ID sensor, which is found in the round button (often referred to as the “home” button) located at the bottom center of the front of the device. The fingerprint sensors found on devices produced by other manufacturers have different names but operate similarly to Touch ID.

c. If a device is equipped with a facial recognition feature, a user may enable the ability to unlock the device through his or her face. For example, Apple offers a

facial recognition feature called “Face ID.” During the Face ID registration process, the user holds the device in front of his or her face. The device’s camera then analyzes and records data based on the user’s facial characteristics. The device can then be unlocked if the camera detects a face with characteristics that match those of the registered face. Facial recognition features found on devices produced by other manufacturers have different names but operate similarly to Face ID.

d. In my training and experience, users of electronic devices often enable the aforementioned biometric features because they are considered to be a more convenient way to unlock a device than by entering a numeric or alphanumeric passcode or password. Moreover, in some instances, biometric features are considered to be a more secure way to protect a device’s contents. This is particularly true when the users of a device are engaged in criminal activities and thus have a heightened concern about securing the contents of a device.

e. As discussed in this affidavit, the FBI has the **Target Device** in its possession. A passcode or password that would unlock the **Target Device** has been provided, however, it has not been confirmed. Thus, if the passcode provided is not correct, law enforcement personnel may not otherwise be able to access the data contained within the device, making the use of biometric features necessary to the execution of the search authorized by this warrant.

f. I also know from my training and experience, as well as from information found in publicly available materials including those published by device manufacturers, that biometric features will not unlock a device in some circumstances even if such

features are enabled. This can occur when a device has been restarted, inactive, or has not been unlocked for a certain period of time. For example, Apple devices cannot be unlocked using Touch ID when (1) more than 48 hours has elapsed since the device was last unlocked or (2) when the device has not been unlocked using a fingerprint for 4 hours *and* the passcode or password has not been entered in the last 156 hours. Biometric features from other brands carry similar restrictions. Thus, in the event law enforcement personnel encounter a locked device equipped with biometric features, the opportunity to unlock the device through a biometric feature may exist for only a short time.

g. Due to the foregoing, if the **Target Device** may be unlocked using one of the aforementioned biometric features, the warrant I am applying for would permit law enforcement personnel to (1) press or swipe the fingers (including thumbs) of **Rigney**, who is reasonably believed by law enforcement to be a user of the device, to the fingerprint scanner of the device; and (2) hold the device in front of the face of **Rigney** and activate the facial recognition feature, for the purpose of attempting to unlock the device in order to search its contents as authorized by this warrant.

### **CONCLUSION**

30. Based on the information set forth in this affidavit, there is probable cause to believe that evidence, fruits, and instrumentalities of violations of 18 U.S.C. § 2252A are presently located within the **Target Device**, more specifically described in Attachment A. Accordingly, I respectfully request that this Court authorize the search of all of the contents of the **Target Device**, including any synchronized applications or incorporated data cards, and to



seize the items specified in Attachment B, which constitute evidence and instrumentalities of violations of 18 U.S.C. § 2252A.



Ingri C. Hartwig, Special Agent  
Federal Bureau of Investigation

Agent sworn and information and signature confirmed via reliable electronic means pursuant to Federal Rule of Criminal Procedure 41(d)(3) on March 22, 2023.



IRMA CARRILLO RAMIREZ  
UNITED STATES MAGISTRATE JUDGE

**ATTACHMENT A**

**DESCRIPTION OF THE TARGET DEVICE TO BE SEARCHED**

The **Target Device** is described as a black Apple iPhone, with assigned phone number (214) 624-2552. The **Target Device** is presently located at the evidence control room of the FBI, Dallas Division, located at One Justice Way, Dallas, Texas, 75220.

This warrant authorizes the forensic examination of the **Target Device** for the purpose of identifying the electronically stored information described in Attachment B.

**ATTACHMENT B**  
**DESCRIPTION OF ITEMS TO BE SEIZED AND SEARCHED**  
**FROM THE TARGET DEVICE**

Contraband, evidence, fruits, and instrumentalities related to possession of or access with intent to view child pornography as defined in 18 U.S.C. § 2256(8), in any form, including, but not limited to:

1. Videos, still images, and other recordings of visual depictions of minors engaged in sexually explicit conduct, as defined in 18 U.S.C. § 2256;
2. Written, typed, or verbal communications by or to **Rigney** that reflect how **Rigney** obtained, received, possessed, accessed with intent to view child pornography, or attempted to do the same;
3. Evidence of mobile applications or other programs used to hide, obtain, access, or store images of child pornography;
4. Evidence of who used, owned, or controlled the **Target Device** at the time the items described in this warrant were created, edited, or deleted, such as logs, registry entries, configuration files, saved usernames and passwords, documents, browsing history, user profiles, email, email contacts, “chat,” instant messaging logs, photographs, and correspondence;
5. Evidence of the times the **Target Device** was used;
6. Passwords, encryption keys, and other access devices that may be necessary to access the **Target Device**, applications on the **Target Device**, or remote storage services;

7. Records of or information about Internet Protocol addresses used by the **Target Device**;

8. Records of or information about the **Target Device's** Internet activity, including firewall logs, caches, browser history and cookies, "bookmarked" or "favorite" web pages, search terms that the user entered into any Internet search engine, and records of user-typed web addresses;

9. Credit card information, including but not limited to bills and payment records related to the use of mobile applications and remote storage;

10. Information or correspondence pertaining to affiliation with any child exploitation websites or social media applications;

11. Any evidence of software that would allow others to control the **Target Device**, such as viruses, Trojan horses, and other forms of malicious software, as well as evidence of the presence or absence of security software designed to detect malicious software; and

12. Evidence of the lack of such malicious software.

This warrant authorizes a review of electronic storage media and electronically stored information seized or copied pursuant to this warrant in order to locate evidence, fruits, and instrumentalities described in this warrant. The review of this electronic data may be conducted by any government personnel assisting in the investigation, who may include, in addition to law enforcement officers and agents, attorneys for the government, attorney support staff, and technical experts. Pursuant to this warrant, the FBI may

deliver a complete copy of the seized or copied electronic data to the custody and control of attorneys for the government and their support staff for their independent review.

During the execution of the search of the **Target Device** described in Attachment A, law enforcement personnel are authorized to (1) press or swipe the fingers (including thumbs) of **Paul Wayne Rigney**, a white male with date of birth 02/16/19XX, and who is currently in federal custody, who is reasonably believed by law enforcement to be a user of the **Target Device**, to the fingerprint scanner of the device; (2) hold the **Target Device** in front of the face of that same individual and activate the facial recognition feature, for the purpose of attempting to unlock the device in order to search the contents as authorized by this warrant.